UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/717,770	11/20/2003	Ling Tony Chen	13768.810.62	8379

47973 7590 07/21/2009

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER	
SHAN, APRIL YING	
ART UNIT	PAPER NUMBER
2435	
MAIL DATE	DELIVERY MODE
07/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/717,770	CHEN, LING TONY	
	Examiner	Art Unit	
	APRIL Y. SHAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 April 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5,8,11,14 and 19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5,8 and 19* is/are rejected.

7)☒ Claim(s) *11 and 14* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The Applicant's amendment, filed 24 April 2009, has been received, entered into the record, and respectfully and carefully considered.

2. As a result of the amendment, claims 1, 5, 8, 11, 14 and 19 have been amended. Claims 2-4, 6-7, 9-10, 12-13, 15-18 and 20-36 are canceled. Claims 1, 5, 8, 11, 14 and 19 are now presented for examination.

3. Any claim objection/rejection not repeated below is withdrawn due to Applicant's amendment.

Response to Arguments

4. Applicant's arguments filed 24 April 2009 have been respectfully and fully considered but they are not persuasive.

In summary, the Applicant argues "Bowe and Jackson fails to teach or suggest the particular computation of the first and second digests by the client and the particular communication of the first and second digests from the client to the server for initial signature computation and for later verification", the examiner respectfully disagrees. Contrary to Applicant's argument, Bowe discloses the client sending first/second data related information and the signature to the server to verify that the data that were stored have not been changed (*A user/client sends a data object to the server and the server generates a digital signature for the data object - e.g. step 210 in fig. 2, abstract, paragraph [0035] and [0054]. Please note data object corresponds to Applicant's first data related information and A client can, at a later time, send the signature back to the*

server for verification – e.g. step verification request & Singed Object in fig. 3, abstract, paragraph [0036] and [0060]) and Jackson et al. discloses *The hashed data string may be referred to as a "message digest." A message digest can be stored for future use, or encrypted and then stored in nonvolatile memory* (e.g. col. 6, lines 49-52), *the shared object code, as well as other data may be verified by first preparing a signature from data. The signature may be prepared by first hashing the data set to create a message digest. The message digest is encrypted via an encryption program utilizing a private/public key algorithm, forming a unique signature. The data and signature are then stored on a mass storage device* (e.g. col. 11, lines 13-22). Further, in order not to repeat herself, the examiner respectfully invites the Applicant to read below 103 rejections, in which the examiner clearly set forth her position/rationale of rejecting newly added claim limitations.

Claim Objections

5. Claims 1, 5, 8, 11, 14 and 19 are objected to because of the following informalities:

As per **claim 1**, "the previously stored signature" is being recited. Since there is no such "previously stored signature" being recited before "the previously stored signature", the examiner assumes "the previously stored signature" is referring to "the client storing…the signature…in the persistent storage of the client". Please clarify.

Any claim not specifically addressed, above, is being objected as incorporating the deficiencies of a claim upon which it depends.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7 The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

8. **Claims 1, 5, 8 and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over Bowe et al. *(U.S. Pub. No. 2003/0093678)* in view of Jackson et al. *(U.S. Patent No. 7,116,782).*

As per **claim 1**, Bowe et al. discloses a method, comprising:

the client *(e.g. client 100 in fig. 2)* sending first data related information *(e.g. data object 210 in fig. 2)* to a server *(e.g. server 120 in fig. 2)* for signature computation *(A user/client sends a data object to the server and the server*

generates a digital signature for the data object - e.g. step 210 in fig. 2, abstract, paragraph [0035] and [0054]. Please note data object corresponds to Applicant's first data related information);

the server, comprising a second computing device *(e.g. server 120 in fig. 2)*, computing a signature for the first data related information by utilizing a secure signing algorithm and a key only known and available for use by the server *(The server generates by performing a hash function and maintains all of the user's keys used for producing a digital signature and the server generates a digital signature for the data object using the private key stored at the server – step 225 in fig. 2, abstract, paragraph [0037]. Please note user's keys generated and maintained by the server correspond to Applicant's a key that is only known and available for the use by the server and as evidenced by fig. 4 and paragraph [0061] that keys to generate a verifying hash are only known and available for use by the server);*

the server sending the signature to the client *(the server then sends the digital signature to the client – e.g. abstract, paragraph [0035]);*

before the data that were stored are subsequently used by the client, the client sending both second data related information and the signature to the server to verify that the data that were stored have not been changed *(A client can, at a later time, send the signature back to the server for verification – e.g. step verification request & Singed Object in fig. 3, abstract, paragraph [0036] and [0060]*

); the server receiving both the second data related information and the signature (e.g. fig. 2 and fig. 3)

the server generating a temporary signature of the second data related information *(e.g. second hash 310 in fig. 3 and step of server generates second hash in fig. 3)* by utilizing the secure signing algorithm *(e.g. hash function in paragraph [0054] and verifying step using a predetermined hash function - claims 19 and 43)* and the key that is only known and available for use by the server *(e.g. verifying step using the private key to generate a comparison value - e.g. claims 19 and 43, par. [0061] and fig. 4);*

the server comparing the temporary signature to the stored signature *(The server generates a second hash using the original data object and compares the hash from the signature with the second hash – e.g. step server compares hashes in fig. 3, paragraph [0040] and [0060]);*

when the temporary signature is equal to the stored signature, sending a positive result to the client *(If the hash values match, the server generates a "valid" verification response, which it sends to the client – e.g. success indicator in fig. 3, paragraph [0040] and [0060]);*

when the temporary signature is not equal to the stored signature, sending a negative result to the client *(The server returns an indicator showing the status of the signature, either valid or invalid – e.g. failure indicator in fig. 3 and paragraph [0060])*;

the client receiving the result from the server *(client receives success/failure indicator from server – e.g. fig. 3);*

Although Bowe et al. discloses *the server then sends the digital signature to the client – e.g. abstract* and *paragraph [0035], a client, at a later time, send the signature back to the server for verification – e.g. step verification request & Singed Object in fig. 3, abstract, paragraph [0036] and [0060] and the server sends success/failure indicator to the client after verification – e.g. fig. 3,* Bowe et al. does not explicitly disclose the data objects are message digests, the client storing both the signature and the data in the persistent storage of the client, and evaluating the result. However, Jackson et al. met the claimed limitations by disclosing *The hashed data string may be referred to as a "message digest." A message digest can be stored for future use, or encrypted and then stored in nonvolatile memory* (e.g. col. 6, lines 49-52), *the shared object code, as well as other data may be verified by first preparing a signature from data. The signature may be prepared by first hashing the data set to create a message digest. The message digest is encrypted via an encryption program utilizing a private/public key algorithm, forming a unique signature. The data and signature are then stored on a mass storage device* (e.g. col. 11, lines 13-22), *a computerized wagering game apparatus in communication with a network server and the data received in the game apparatus maybe verified via a digital signature employing hashing functions before execution that errors will be caught at the time they occur rather than when the data is loaded or reloaded (e.g. fig. 2, col. 7, line 67 - col. 8, line 6. Please note computerized wagering game*

apparatus corresponds to Applicant's client and before execution to catch error corresponds to Applicant's evaluating the result, when the result is positive, the client using the data and when the result is negative, the client not using the data) and the data and signature are then stored on hard drive, CD-ROM, flash disk (e.g. col. 11, lines 20 – 22. Please note hard drive, CD-ROM and flash disk correspond to Applicant's persistent storage).

Bowe et al. - Jackson et al. are analogous art because they are from a similar field of endeavor in using digital signature to verify data in a client-server environment. Thus, it would have been obvious to a person with ordinary skill in the art, at the time of invention, to combine the teachings of Jackson's the data objects are message digests, the client storing both the signature and the data in the persistent storage of the client, and evaluating the result; with Bowe et al. The motivation of doing so would have been message digest is a hashed data string can be stored for future use and to advantageously read/write, yet retains information stored upon power down and to improve or ensure security *(e.g. Jackson et al. – col. 1, lines 18 -20, col. 6, lines 49-52 and col. 9, lines 50-52).*

As per **claim 5**, Bowe et al. - Jackson et al. discloses the method as applied above in claim 1. Bowe et al. – Jackson et al. further discloses wherein the digest related information comprises a digest of the data calculated by the client using a one-way hash function and the data *(The server creates a signature by*

performing a hash function on the data object - e.g. paragraph [0037] of Bowe et al. and col. 9, lines 50-52 and col. 11, lines 13-22 of Jackson et al.*)*, and the second digest comprises a digest of the stored data calculated by the client using a one-way hash function and the stored data *(Server generates second hash in fig. 3 and paragraph [0060] of Bowe et al. and col. 9, lines 50-52 and* col. 11, lines 13-22 of Jackson et al.*)*.

As per **claim 8**, Bowe et al. - Jackson et al. discloses the method as applied above in claim 5. Bowe et al. – Jackson et al. further discloses wherein the first digest (e.g. *and col. 9, lines 50-52 and* col. 11, lines 13-22 of Jackson et al.) further comprises: a signer identification (SID) for the client, the SID uniquely identifying the client and not being controlled by an operator of the client *(The signature property field contains a client identifier – e.g. paragraph [0039]. Please note client identifier corresponds to Applicant's signer identification (SID) of Bowe et al.).*

As per **claim 19**, Bowe et al. - Jackson et al. disclose method of steps as applied above in claim 1. Therefore, Bowe et al. - Jackson et al. 1discloses the claimed machine readable instructions stored on a memory medium for carrying out the method of steps.

Allowable Subject Matter

9. **Claims 11 and 14** would be allowable if rewritten to overcome the claim objections, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to APRIL Y. SHAN whose telephone number is (571)270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/April Y Shan/
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435